REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant acknowledges the Examiner's indication of the allowability of claims 21, 26, 36, and 47 if rewritten in independent form.

Amendments to the Claims

Claim 27 is amended inserting "secret" between "said" and "private" on line 3 of the claim.

Claim 38 is amended inserting "private" between "secret" and "key" on line 3 of the claim and removing "bP" on line 9 of the claim.

No new subject matter is believed to have been added by way of these amendments.

Claim Rejections – 35 U.S.C §112

Claims 27 and 38 have been rejected under 35 U.S.C §112, second paragraph for being indefinite. Claims 27 and 38 are amended as indicated above and are believed to comply with 35 U.S.C §112, second paragraph.

Claim Rejections – 35 U.S.C §102(e)

Claims 7-8, 23-24, 27, 38 and 48 have been rejected under 35 U.S.C §102(e) as being anticipated by U.S. Patent No. 6,336,188 to Blake-Wilson et al. Applicant respectfully traverses the rejections as follows.

The present application describes and claims a method for generating session keys using MACs, whereby the MACs are computed using one of a pair of secret keys. The secret keys are generated by each correspondent, and the MACs are exchanged and verified in order to establish a pair of session keys. A first of the secret keys is used in generating the MACs, and the other is used in generating the session keys.

For example, in claim 7, the first correspondent generates a pair of secret keys at step c), and the second correspondent generates the secret keys at step f). The first of the secret keys is used to generate first and second MACs at steps g) and h); and the second of the secret keys is used to compute a pair of session keys at step k).

Blake-Wilson teaches an authenticated key agreement scheme, wherein authentication

messages are computed from a shared secret. The shared secret is computed by each correspondent using the respective correspondent's private key and the other correspondent's public key using a function H. The authentication messages are generated, exchanged, and verified to establish a short term shared secret. Blake-Wilson does not teach generating first and second MACs using one of a pair of generated secret keys, nor generating a pair of session keys using the other of the pair of generated secret keys, but rather Blake-Wilson teaches generating a single shared secret using private and public keys.

Regarding claim 7, the Examiner relies on col. 2, lines 4-6 of Blake-Wilson as teaching step c). However, This passage clearly indicates that only "a long term shared secret key k'" is derived, not a pair of secret keys. Since Blake-Wilson does not teach generating a pair of secret keys, he cannot possibly teach using one of a pair of keys to generate MACs and the other to generate session keys.

The Examiner relies on col. 2 lines 11-20 as teaching steps g), h), and i). This passage teaches, in part, computing an authenticated message using the long term shared secret computed at lines 4-6. Therefore, for the sake of argument, Blake-Wilson may at most teach generating a MAC using a single shared secret key. However, since Blake-Wilson does not teach generating a pair of secret keys, he cannot teach using a second secret key to compute a pair of session keys (e.g. step k)). In fact, Blake-Wilson is entirely silent as to utilizing such a second secret key. The Examiner relies on col. 2, lines 23-26 as teaching step k). However, this step clearly teaches computing a short term shared secret using a private and public key, not using a second generated secret key to generate a pair of session keys. In fact, this step does not even teach a pair of keys being computed, but only one.

Accordingly, Blake-Wilson does not teach generating first and second MACs using one of a pair of generated secret keys, nor generating a pair of session keys using the other of the pair of generated secret keys, and as such, cannot anticipate claim 7. Claims 8-26 being ultimately dependent on claim 7 are also believed to distinguish over Blake-Wilson.

Claims 27, 38 and 48 each involve the use of a pair of secret keys. Therefore, Blake-Wilson also cannot anticipate claims 27, 38 and 48. Claims 28-37 and 39-47 being ultimately dependent on either claim 27 or 38 are also believed to distinguish over Blake-Wilson.

Claim Rejections – 35 U.S.C §103(a)

Claims 9-11, 13-14, 22, 28-29 and 39-40 have been rejected under 35 U.S.C §103(a) as being unpatentable over Blake-Wilson in view of US Patent No. 5,153,919 to Reeds, III et al. Applicant respectfully traverses these rejections as follows.

Reeds, III does not teach a pair of secret keys as required by independent claims 7, 27, 38 and 48. Therefore, Reeds, III does not teach what is missing from Blake-Wilson as discussed above, and as such claims 9-11, 13-14, 22, 28-29 and 39-40 are believed to clearly and patentably distinguish over Blake-Wilson in view of Reeds, III.

Claim 12 has been rejected under 35 U.S.C §103(a) as being unpatentable over Blake-Wilson in view of US Patent No. 5,784,463 to Chen et al. Applicant respectfully traverses this rejection as follows.

Chen does not teach a pair of secret keys as required by independent claims 7, 27, 38 and 48. Therefore, Chen does not teach what is missing from Blake-Wilson as discussed above, and as such claim 12 is believed to clearly and patentably distinguish over Blake-Wilson in view of Chen.

Claims 15-16, 30-31, and 41-42 have been rejected under 35 U.S.C §103(a) as being unpatentable over Blake-Wilson in view of Reeds, III, and further in view of US Reissue Patent No. Re.36,946 to Diffie et al. Applicant respectfully traverses these rejections as follows.

Neither Reeds, III nor Diffie teach a pair of secret keys as required by independent claims 7, 27, 38 and 48. Therefore, neither Reeds, III nor Diffie teach what is missing from Blake-Wilson as discussed above, and as such claims 15-16, 30-31 and 41-42 are believed to clearly and patentably distinguish over Blake-Wilson in view of Reeds, III, in further view of Diffie.

Claims 17-18, 32-33, and 43-44 have been rejected under 35 U.S.C §103(a) as being unpatentable over Blake-Wilson in view of Reeds, III, and further in view of US Patent No. 5,883,960 to Maruyama et al. Applicant respectfully traverses these rejections as follows.

Neither Reeds, III nor Maruyama teach a pair of secret keys as required by independent claims 7, 27, 38 and 48. Therefore, neither Reeds, III nor Maruyama teach what is missing from Blake-Wilson as discussed above, and as such claims 17-18, 32-33 and 43-44 are believed to clearly and patentably distinguish over Blake-Wilson in view of Reeds, III, in further view of Maruyama.

Claims 19-20, 34-35, and 45-46 have been rejected under 35 U.S.C §103(a) as being unpatentable over Blake-Wilson in view of Reeds, III, and further in view of US Patent No. 6,260,147 to Quick, Jr.. Applicant respectfully traverses these rejections as follows.

Neither Reeds, III nor Quick, Jr. teach a pair of secret keys as required by independent claims 7, 27, 38 and 48. Therefore, neither Reeds, III nor Quick, Jr. teach what is missing from Blake-Wilson as discussed above, and as such claims 19-20, 34-35 and 45-46 are believed to clearly and patentably distinguish over Blake-Wilson in view of Reeds, III, in further view of Maruyama.

Claims 25 and 37 have been rejected under 35 U.S.C §103(a) as being unpatentable over Blake-Wilson in view of US Patent No. 6,209,093 to Venkatesan et al. Applicant respectfully traverses this rejection as follows.

Venkatesan does not teach a pair of secret keys as required by independent claims 7, 27, 38 and 48. Therefore, Venkatesan does not teach what is missing from Blake-Wilson as discussed above, and as such claim 12 is believed to clearly and patentably distinguish over Blake-Wilson in view of Venkatesan.

Summary

In view of the foregoing, Applicant respectfully submits that claims 7-48 clearly and patentably distinguish over the prior art cited by the Examiner, and as such are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

Ralph A. Dowell
Agent for Applicant
Registration No. 26,868

Date: December 14, 2005